An Algorithm for NTRU Problems and Cryptanalysis of the GGH Multilinear Map without a Low Level Encoding of Zero

Jung Hee Cheon, Jinhyuck Jeong, Changmin Lee

Seoul National University (SNU), Republic of Korea

Abstract. Let $\boldsymbol{f}$ and $\boldsymbol{g}$ be polynomials of a bounded Euclidean norm in the ring $\mathbb{Z}[X]/\langle X^n+1\rangle$. Given the polynomial $[\boldsymbol{f}/\boldsymbol{g}]_q \in \mathbb{Z}_q[X]/\langle X^n+1\rangle$, the NTRU problem is to find $\boldsymbol{a},\ \boldsymbol{b} \in \mathbb{Z}[X]/\langle X^n+1\rangle$ with a small Euclidean norm such that $[\boldsymbol{a}/\boldsymbol{b}]_q = [\boldsymbol{f}/\boldsymbol{g}]_q$. We propose an algorithm to solve the NTRU problem, which runs in $2^{O(\log^2 \lambda)}$ time when $\|\boldsymbol{g}\|, \|\boldsymbol{f}\|$, and $\|\boldsymbol{g}^{-1}\|$ are within some range. The main technique of our algorithm is the reduction of a problem on a field to one in a subfield. Recently, the GGH scheme, the first candidate of a (approximate) multilinear map, was found to be insecure by the Hu–Jia attack using low-level encodings of zero, but no polynomial-time attack was known without them. In the GGH scheme without low-level encodings of zero, our algorithm can be directly applied to attack this scheme if we have some top-level encodings of zero and a known pair of plaintext and ciphertext. Using our algorithm, we can construct a level-0 encoding of zero and utilize it to attack a security ground of this scheme in the quasi-polynomial time of its security parameter using the parameters suggested by [GGH13].

Keywords: NTRU, GGH Multilinear Maps, Ideal Lattice, Shortest Vector Problem

1 Introduction

The NTRU problem is to find a pair of small polynomials whose ratio matches a given ratio of two small polynomials [HPS98]. After the introduction of the security of the public-key encryption scheme NTRU, it has been assumed that this NTRU problem is difficult to solve—the so-called NTRU assumption—and has been used for the security grounding of various cryptographic schemes such as signature schemes [HHGP+03,DDLL13], fully homomorphic encryption scheme [LATV12,BLLN13], and candidates for cryptographic multilinear maps [GGH13,LSS14,ACLL14]. As it has not been broken until now, the NTRU assumption has received more attention as a candidate for post-quantum public-key cryptosystems. A variant of NTRU problem can be stated as follows:

Problem 1 (A variant of the NTRU problem)
Let $\phi_n(X) \in \mathbb{Z}[X]$ be a polynomial of degree n, $q \in \mathbb{Z}$ be an integer, and D, N, and B be real numbers. The NTRU problem $NTRU_{\phi_n,q,D,N,B}$ is to find

$\boldsymbol{a}$, $\boldsymbol{b}$ $\in R := \mathbb{Z}[X]/\langle\phi_n(X)\rangle$ with a Euclidean norm smaller than B such that $[\boldsymbol{b}/\boldsymbol{a}]_q = \boldsymbol{h}$ for given a polynomial $\boldsymbol{h} = [\boldsymbol{f}/\boldsymbol{g}]_q$, where $\boldsymbol{f}$ and $\boldsymbol{g}$ are sampled from R and have Euclidean norms bounded by D and N, respectively.

In the original NTRU problem, $\boldsymbol{f}$ and $\boldsymbol{g}$ are sampled from some distribution of R [HPS98, Section 1]. [1] We consider this variant version to attack multilinear maps [GGH13].

In this paper, we propose a polynomial-time reduction from $NTRU_{\phi_n,q,D,N,B}$ into $NTRU_{\phi_{n/2},q,D_1,N_1,B_1}$, where $\phi_n = X^n + 1$, $B = \min\{\frac{q}{2D\sqrt{n}}, \frac{q}{2N\sqrt{n}}\}$, $D_1 = D^2\sqrt{n/2}$, $N_1 = 2ND\sqrt{n/2}$, and $B_1 = \min\{\frac{q}{2D_t\sqrt{n}}, \frac{q}{2N_t\sqrt{n}}, \frac{q}{2nN^2\|\boldsymbol{g}^{-1}\|\sqrt{n}}\}$ for a power n of 2. Our algorithm is to reduce the problem defined over a ring $\mathbb{Z}[X]/\langle X^n + 1\rangle$ to one over a subring $\mathbb{Z}[X]/\langle X^{n/2} + 1\rangle$. After repeated applications, we then use lattice reduction algorithms to find a short element. Since the latter has a smaller dimension, lattice reduction algorithms require a lower running time to produce a short element, which results in an algorithm for the NTRU problem. The algorithm runs in $2^{O(\log^2 \lambda)}$ time when $\|\boldsymbol{g}\|, \|\boldsymbol{f}\|$ and $\|\boldsymbol{g}^{-1}\|$ are within some range. For example, when $n = \lambda^2$ and $\log q = \lambda$, the running time is quasi-polynomial in λ. However, when $n = \lambda^3$ and $\log q = \lambda$, the running time is still an exponential time in λ. As an application of our work, we propose an attack of GGH multilinear maps [GGH13] without any low-level encodings of zero. GGH maps were proposed by Garg *et al.* and broken by a so-called zeroizing attack by Hu and Jia [HJ15]. Since their attack extensively utilizes low-level encodings of zero, it does not work without them, and no polynomial-time attack was known without them until recently (refer to the "Related work" subsection for the concurrent and independent works on this problem). Our algorithm can be directly applied to construct a level-0 encoding of zero, even when we are not given any low-level encodings of zero. We can then utilize them to attack the GGH scheme without low-level encodings of zero in the polynomial time of its security parameter. Our GGH attack requires a known pair of plaintext and ciphertext, some top-level encodings of zero, and the public parameters.

Technical overview. A natural approach for the NTRU problem is to convert it into a shortest vector problem (SVP) on an ideal lattice. Let $\phi_n(X) = X^n + 1$ when n is a power of 2. For any polynomial $\boldsymbol{h} = [\boldsymbol{f}/\boldsymbol{g}]_q = \sum_{i=0}^{n-1} h_i X^i \in R := \mathbb{Z}[X]/\langle X^n + 1\rangle$, one may consider it as a vector $(h_0, \cdots, h_{n-1})^T$. Then, the product $\boldsymbol{gh} = \sum_{i=0}^{n-1} g_i X^i \boldsymbol{h}$ of the two polynomials $\boldsymbol{h}$ and $\boldsymbol{g}$ in R is contained in the lattice $\mathcal{M}_{\boldsymbol{h}}$ generated by $\{\boldsymbol{h}, X\boldsymbol{h}, \cdots, X^{n-1}\boldsymbol{h}\}$. We aim to obtain an element $\tilde{\boldsymbol{g}} \in \mathbb{Z}[X]/\langle\phi(X)\rangle$ satisfying $\|\tilde{\boldsymbol{g}}\|$ and $\|[\tilde{\boldsymbol{g}}\boldsymbol{h}]_q\|$ are small. To obtain such a $\tilde{\boldsymbol{g}} \in \mathbb{Z}[X]/\langle\phi(X)\rangle$, one can naturally contemplate the following column lattice:

$$\Lambda_{\boldsymbol{h}} = \begin{pmatrix} I & 0 \\ M_{\boldsymbol{h}} & qI \end{pmatrix},$$

[1] $\boldsymbol{f}$ and $\boldsymbol{g}$ are sampled to satisfy that $\boldsymbol{f} = p\boldsymbol{f}'$ and $\boldsymbol{g} - 1 = p\boldsymbol{g}'$ for a small integer p and the polynomials $\boldsymbol{f}'$ and $\boldsymbol{g}'$ in R with the coefficients in $\{-1, 0, 1\}$.

where I is the identity matrix of size n, and $M_{\boldsymbol{h}}$ is a basis matrix of $\mathcal{M}_{\boldsymbol{h}}$ juxtaposed by $\{\boldsymbol{h}, X\boldsymbol{h}, \cdots, X^{n-1}\boldsymbol{h}\}$. Given a lattice vector $\boldsymbol{u} = (u_0, \cdots, u_{2n-1})^T$ of Λ_f satisfying $|u_i| < q/2$ for $n \leq i \leq 2n-1$, we take $\boldsymbol{g}' = \sum_{i=0}^{n-1} u_i X^i$ and $\boldsymbol{f}' = \sum_{i=0}^{n-1} u_{n+i} X^i$ so that $\boldsymbol{f}' = [\boldsymbol{g}'\boldsymbol{h}]_q$ and $\boldsymbol{h} = [\boldsymbol{f}'/\boldsymbol{g}']_q$. Therefore, if one can find a small lattice point $\boldsymbol{u}$ such that $\sqrt{\sum_{i=0}^{n-1} u_i} \leq \frac{q}{2\|\boldsymbol{f}\|\sqrt{n}}$ and $\sqrt{\sum_{i=n}^{2n-1} u_i} \leq \frac{q}{2\|\boldsymbol{g}\|\sqrt{n}}$, it becomes a solution of $NTRU_{\phi,q,D,N,B}$. However, the dimension $2n$ of the lattice is too large for most applications, which is the origin of the difficulty of the NTRU problem. To overcome this obstacle, we consider a subfield K_m of $K_0 := \mathbb{Q}[X]/\langle X^n + 1\rangle$ with the extension degree m and the trace of $f \in K_0$ over K_m:

$$\mathrm{Tr}(\boldsymbol{h}) = \left[\sum_{i=1}^{m} \sigma_i(\boldsymbol{h})\right]_q = \left[\sum_{i=1}^{m} (\sigma_i(\boldsymbol{f}) \prod_{j \neq i} \sigma_j(\boldsymbol{g})) / \prod_{i=1}^{m} \sigma_i(\boldsymbol{g})\right]_q .$$

Since the numerator and denominator are elements in K_m bounded by $m\|\boldsymbol{f}\| \cdot \|\boldsymbol{g}\|^{m-1} n^m$ and $\|\boldsymbol{g}\|^m n^m$, respectively, if they are smaller than q, we can construct another instance of the NTRU problem on K_m where the dimension of $\Lambda_{\mathrm{Tr}(\boldsymbol{h})}$ is that of $\Lambda_{\boldsymbol{h}}$ divided by m. By optimizing m such that finding a small vector on the reduced lattice is possible with BKZ algorithm, one can reach our results.

Multilinear maps. After Boneh and Silverberg [BS02] suggested the concept of cryptographic multilinear maps and their applications such as multipartite Diffie–Hellman and efficient broadcast encryption in 2002, the construction of cryptographic multilinear maps has been a longstanding open question. In 2013, approximate cryptographic multilinear maps were first proposed by Garg, Gentry, and Halevi (GGH) [GGH13]. Not much later, second and third cryptographic multilinear maps were suggested by Coron, Lepoint, and Tibouchi (CLT) [CLT13], and Gentry, Gorbunov, and Halevi [GGH15], respectively. However, none of these maps have a reduction to a standard difficultly problem such as the subset sum problem. In fact, the first two schemes with low-level encodings of zero are known to be insecure [CHL$^+$15,HJ15] via the so-called zeroizing attack. The last candidate is also broken [Cor15]. Although the fixed scheme of [CLT13] was proposed by the same authors of [CLT15] to resist the zeroizing attack against the CLT scheme, it was also shown to be insecure [CLR15]. On the other hand, both the [GGH13] and [CLT13] schemes without any encodings of zero, which are used as basic tools for constructing applications such as indistinguishable obfuscations, have still not been analyzed.

Related work. In 2002, a technique was suggested to reduce the dimension of an ideal lattice by Gentry and Szydlo [GS02]. They consider a subring of a given ring $\mathbb{Z}[X]/\langle X^n - 1\rangle$ consisting of the fixed elements by the ring automorphism

$\sigma : X \mapsto X^{n-1}$. This techique, however, has no guarantee that one can apply it repeatedly to reduce the dimension more efficiently.

Recently, for GGH multilinear maps without encodings of zero, two more concurrent and independent cryptanalytic works have been announced simultaneously, which can overcome the previous flaw: one by Albrecht, Bai, and Ducas [MA16] and the other by Miles, Sahai, and Zhandry [MSZ16]. The first introduces a very similar reduction from $NTRU_{\phi_n,q,D,N,B}$ to $NTRU_{\phi_{n/2},q,D_1,N_1,B_1}$. They provided a rich analysis of the NTRU-like homomorphic encryptions LTV [LATV12] and YASHE [BLLN13] and GGH multilinear maps with some implementations. Using the norm function instead of the trace function in our algorithm, they proposed a quantum-polynomial-time or subexponential-time attack on GGH without low-level encodings of zero. In our work, we can achieve the same, but slightly better, results using the trace function. Moreover, through our new approach, we can obtain an algorithm to attack GGH scheme without low-level encodings of zero in quasi-polynomial time.

The second introduced a polynomial-time attack algorithm against the GGH multilinear maps, the so-called *annihilation attack*. Using nonlinear polynomials, it also leads to a polynomial-time break of the GGH scheme without low-level encodings of zero.

Organization. In Section 2, we introduce some notation and preliminary information related to ideal theory and Galois theory. In Section 3, we state some useful properties and their proofs used to solve the $NTRU$ problem. In Section 4, we briefly explain the GGH scheme and present our algorithm for attacking the GGH scheme using our theorem.

2 Preliminaries

Notation. For an integer q, we use the notation $\mathbb{Z}_q := \mathbb{Z}/(q\mathbb{Z})$ and $[R]_q := \mathbb{Z}_q[X]/\langle X^n+1\rangle = R/qR$. We denote the number in $\mathbb{Z}_q$ within the range $\left(-\frac{q}{2}, \frac{q}{2}\right]$ by $(x \bmod q)$ or $[x]_q$, which is congruent to x modulo q. For $\boldsymbol{u} = \sum_{i=0}^{n-1} u_i X^i \in R$, $[\boldsymbol{u}]_q = \sum_{i=0}^{n-1} [u_i]_q X^i$ and $\|\boldsymbol{u}\|$ denote the Euclidean norm of $\boldsymbol{u}$.

We define $\iota : \mathbb{Z}_q \longrightarrow \mathbb{Z}$ by $[x]_q \in \mathbb{Z}_q \mapsto x \in \mathbb{Z}$ for $-\frac{q}{2} < x \leq \frac{q}{2}$. We extend this map to $[R]_q$ by applying it to each coefficient. By abuse of notation, we omit ι unless it will be confused when identifying $[x]_q \in \mathbb{Z}_q$ with an integer x when $-\frac{q}{2} < x \leq \frac{q}{2}$.

Throughout this paper, we assume that an integer n is a power of 2. Then, $K := \mathbb{Q}[X]/\langle X^n+1\rangle$ is a number field with the ring of integers $R := \mathbb{Z}[X]/\langle X^n+1\rangle$. In particular, K is a Galois extension of $\mathbb{Q}$, and we denote the Galois group of K over $\mathbb{Q}$ by $\mathrm{Gal}(K/\mathbb{Q})$. As in the technical overview, for any polynomial $\boldsymbol{h} = \sum_{i=0}^{n-1} h_i X^i \in K$, we consider it to be a column vector $(h_0, \cdots, h_{n-1})^T$. When we need an inverse of an element $\boldsymbol{a} \in R$, we usually consider the inverse in K

with the notation $\boldsymbol{a}^{-1}$. If we want to consider it in $[R]_q$ and not in K, then we denote it by $\left[\boldsymbol{a}^{-1}\right]_q$. We use bold letters to denote vectors or ring elements in $\mathbb{Z}^n$ or R.

Ideal lattice. An n-dimension full-rank lattice $\mathcal{M} \subset \mathbb{R}^n$ is the set of all $\mathbb{Z}$-linear combinations of n linearly independent vectors. Let $\det(\mathcal{M})$ denote the determinant of the lattice $\mathcal{M}$. For an element $\boldsymbol{g} \in R$, we denote the principal ideal in R generated by $\boldsymbol{g}$ by $\langle \boldsymbol{g} \rangle$, whose basis consists of $\{\boldsymbol{g}, X\boldsymbol{g}, \ldots, X^{n-1}\boldsymbol{g}\}$. By identifying a polynomial $\boldsymbol{g} = \sum g_i X^i \in R$ with a vector $(g_{n-1}, g_{n-2}, \ldots, g_0)^T$ in $\mathbb{Z}^n$, we can apply lattice theory to the algebraic ring R and algebraic ring theory to the ideal lattice $\langle \boldsymbol{g} \rangle$. For a polynomial $\boldsymbol{u} \in R$ and a basis $\mathcal{B} := \{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\}$, we denote the reduction of $\boldsymbol{u}$ modulo the fundamental region of lattice $\mathcal{B}$ by $\boldsymbol{u} \bmod \mathcal{B}$; that is, $\boldsymbol{u} \bmod \mathcal{B}$ is the unique representation of $\boldsymbol{u} \in R$ such that $\boldsymbol{u} - (\boldsymbol{u} \bmod \mathcal{B}) \in \mathcal{B}$ and $\boldsymbol{u} \bmod \mathcal{B} = \sum_{i=0}^{n-1} \alpha_i \boldsymbol{b}_i$ for $\alpha_i \in (-1/2, 1/2]$. For the polynomials $\boldsymbol{u}, \boldsymbol{v} \in R$, we use the notation $\boldsymbol{u} \bmod \boldsymbol{v}$ as $\boldsymbol{u} \bmod \mathcal{V}$, where $\mathcal{V}$ is a basis $\{\boldsymbol{v}, X\boldsymbol{v}, \ldots, X^{n-1}\boldsymbol{v}\}$. By the definition of $\boldsymbol{u} \bmod \boldsymbol{v}$, it is of the form $\sum_{i=0}^{n-1} \alpha_i X^i \boldsymbol{v}$ for $\alpha_i \in (-1/2, 1/2]$. Hence, the size of its Euclidean norm is bounded by $\sum_{i=0}^{n-1} \|X^i \boldsymbol{v}\|/2 = \sum_{i=0}^{n-1} \|\boldsymbol{v}\|/2 = \frac{n}{2}\|\boldsymbol{v}\|$. Next, we introduce some useful lemmas related to ideal lattices.

Lemma 1 *For any $\boldsymbol{a}, \boldsymbol{b} \in R = \mathbb{Z}[X]/\langle X^n + 1 \rangle$, $\|\boldsymbol{ab}\| \leq \|\boldsymbol{a}\| \cdot \|\boldsymbol{b}\| \cdot \sqrt{n}$.*

Proof. The k-th coefficient of $\boldsymbol{ab}$ is of the form $\sum_{i+j=k} a_i b_j - \sum_{i+j=n+k} a_i b_j$. By the Cauchy–Schwartz inequality, it is smaller than $\|\boldsymbol{a}\| \cdot \|\boldsymbol{b}\|$. Since each coefficient is smaller than $\|\boldsymbol{a}\| \cdot \|\boldsymbol{b}\|$, $\|\boldsymbol{ab}\| \leq \|\boldsymbol{a}\| \cdot \|\boldsymbol{b}\| \cdot \sqrt{n}$.

Lemma 2 *Let $\boldsymbol{g}$ be an element of $\mathbb{Z}[X]/\langle X^n + 1 \rangle$ and $\boldsymbol{f} \in \mathbb{Z}[X]/\langle X^n + 1 \rangle$ be a relative prime to $\boldsymbol{g}$. If $\boldsymbol{c} \in \mathbb{Z}[X]/\langle X^n + 1 \rangle$ satisfies $\|\boldsymbol{c}\| < q/(2\|\boldsymbol{f}\|\sqrt{n})$ and $\|[\boldsymbol{c} \cdot \boldsymbol{f} \cdot \boldsymbol{g}^{-1}]_q\| < q/(2\|\boldsymbol{g}\|\sqrt{n})$, then $\boldsymbol{c}$ is contained in the ideal $\langle \boldsymbol{g} \rangle$.*

Proof. Let $\boldsymbol{w} := [\boldsymbol{c} \cdot \boldsymbol{f} \cdot \boldsymbol{g}^{-1}]_q$. Then, $[\boldsymbol{gw}]_q = [\boldsymbol{cf}]_q$. Since $\|\boldsymbol{w}\| < q/(2\|\boldsymbol{g}\|\sqrt{n})$, we have $\|\boldsymbol{gw}\| \leq \|\boldsymbol{g}\| \cdot \|\boldsymbol{w}\| \cdot \sqrt{n} \leq q/2$ and $\|\boldsymbol{cf}\| \leq \|\boldsymbol{c}\| \cdot \|\boldsymbol{f}\| \cdot \sqrt{n} \leq q/2$. Therefore, $\boldsymbol{gw} = \boldsymbol{cf}$ in $\mathbb{Z}[X]/\langle X^n + 1 \rangle$. Because $\boldsymbol{cf} \in \langle \boldsymbol{g} \rangle$ and $\boldsymbol{f}$ is a relative prime to $\boldsymbol{g}$, we can conclude $\boldsymbol{c} \in \langle \boldsymbol{g} \rangle$.

Using Lemma 2, if one can find $\boldsymbol{c}$ that satisfies Lemma 2, $\boldsymbol{c}$ is of the form $\boldsymbol{c} = \boldsymbol{dg}$ for some small $\boldsymbol{d} \in \mathbb{Z}[X]/\langle X^n + 1 \rangle$. Then, by multiplying it by $[\boldsymbol{fg}^{-1}]_q$, one can obtain a small multiple of $\boldsymbol{f}$, $\boldsymbol{df}$. Hence, $\boldsymbol{df}$ and $\boldsymbol{dg}$ become a solution of the NTRU problem.

Gaussian distribution. Given $\sigma > 0$, the discrete Gaussian distribution over the set L with zero mean is defined as $\mathcal{D}_{L,\sigma}(x) = \rho_\sigma(x)/\rho_\sigma(L)$ for any $x \in L$, where $\rho_\sigma(x) = exp(-\pi\|x\|^2/\sigma^2)$ and $\rho_\sigma(L) = \sum_{x \in L} \rho_\sigma(x)$. We use the notation

$a \leftarrow \mathcal{D}$ to denote the choice of an element a according to the distribution of $\mathcal{D}$.

Norm and trace of a field For a finite extension K of a field F, the trace $\mathrm{Tr}_{K/F}(\alpha)$ and norm $\mathrm{N}_{K/F}(\alpha)$ of $\alpha \in K$ over F are defined as the trace and determinant of the linear transformation M_α that maps $x \in K$ to $\alpha x \in K$, respectively, i.e., $\mathrm{Tr}_{K/F}(\alpha) = \sum a_{i,i}$ and $\mathrm{N}_{K/F}(\alpha) = \det(a_{i,j})$, where $a_{i,j}$ is the matrix for M_α with respect to any basis of K over F. The map $\mathrm{Tr}_{K/F}$ and $\mathrm{N}_{K/F}$ satisfy the following properties:

(1) $\mathrm{Tr}_{K/F}(\alpha) = \sum_{\sigma \in Gal(K/F)} \sigma(\alpha)$ and $\mathrm{N}_{K/F}(\alpha) = \prod_{\sigma \in Gal(K/F)} \sigma(\alpha)$ if K is a Galois extension of F
(2) $\mathrm{Tr}_{K/F}(\alpha+\beta) = \mathrm{Tr}_{K/F}(\alpha) + \mathrm{Tr}_{K/F}(\beta)$, $\mathrm{N}_{K/F}(\alpha\beta) = \mathrm{N}_{K/F}(\alpha)\mathrm{N}_{K/F}(\beta)$
(3) $\mathrm{Tr}_{K/F}(a \cdot \alpha) = a \cdot \mathrm{Tr}_{K/F}(\alpha)$, $\mathrm{N}_{K/F}(a \cdot \alpha) = a^{[K:F]} \cdot \mathrm{N}_{K/F}(\alpha)$
(4) $\mathrm{Tr}_{K/F}(a) = [K:F] \cdot a$, $\mathrm{N}_{K/F}(a) = a^{[K:F]}$

for $\alpha, \beta \in K$ and $a \in F$.

3 Main Theorem

In this section, we discuss how the NTRU problem with a given input $[\boldsymbol{f}/\boldsymbol{g}]_q$ is reduced to the NTRU problem with an input whose denominator and numerator have half of the degree of $\boldsymbol{f}$ and $\boldsymbol{g}$. Throughout this section, let $n = 2^s$ and denote $\mathbb{Q}[X^{2^t}]/\langle X^n+1\rangle$ and $\mathbb{Z}[X^{2^t}]/\langle X^n+1\rangle$ by K_t and R_t, respectively, with $0 \le t \le s$. Note that $K_s := \mathbb{Q} \le K_{s-1} \le \cdots \le K_0 = \mathbb{Q}[X]/\langle X^n+1\rangle$, where $A \le B$ denotes that A is a subfield of B. Since K_0 is a Galois extension field of K_1 with a degree of 2, $\mathrm{Gal}(K_0/K_1)$ is a group of order 2. That is, $\mathrm{Gal}(K_0/K_1) = \{id, \sigma\}$, satisfying $\sigma(X) = -X$; therefore, $\sigma^2 = id$, where id is the identity map. For an element $\boldsymbol{h}, \boldsymbol{g} \in R \subset K_0$, the following elements are contained in $R_1 \subset K_1$:

$$\begin{aligned} Tr_{K_0/K_1}(\boldsymbol{h}) &= \boldsymbol{h} + \sigma(\boldsymbol{h}), \\ N_{K_0/K_1}(\boldsymbol{h}) &= \boldsymbol{h} \cdot \sigma(\boldsymbol{h}), \\ Tr_{K_0/K_t}(\boldsymbol{h}\sigma(\boldsymbol{g})) &= \boldsymbol{h}\sigma(\boldsymbol{g}) + \sigma(\boldsymbol{h})\boldsymbol{g}, \end{aligned}$$

since they are fixed by $\mathrm{Gal}(K_0/K_1)$. Note that these elements have only $n/2$ terms, and the last one lies in $2 \cdot R_1$. Generally, for $0 < t \le s$, K_0 is a Galois extension field of K_t with a degree of 2^t and the Galois group $G_t := \mathrm{Gal}(K_0/K_t) = \{\sigma_0 = id, \sigma_1, \ldots, \sigma_{2^t-1}\}$. For an element $\boldsymbol{h}, \boldsymbol{g} \in R \subset K_0$, the following elements are contained in $R_t \subset K_t$:

$$\begin{aligned} &\sum_{i=0}^{2^t-1} \sigma_i(\boldsymbol{h}) = \boldsymbol{h} + \sigma_1(\boldsymbol{h}) + \cdots + \sigma_{2^t-1}(\boldsymbol{h}), \\ &\prod_{i=0}^{2^t-1} \sigma_i(\boldsymbol{h}) = \boldsymbol{h} \cdot \sigma_1(\boldsymbol{h}) \cdot \cdots \cdot \sigma_{2^t-1}(\boldsymbol{h}), \\ &Tr_{K_0/K_t}(\boldsymbol{h}\sigma_1(\boldsymbol{g})\sigma_2(\boldsymbol{g}) \cdots \sigma_{2^t-1}(\boldsymbol{g})), \end{aligned}$$

since they are fixed by $\mathrm{Gal}(K_0/K_t)$. Moreover, these elements have only $n/2^t$ terms, and the last one lies in $2^t \cdot R_t$. Using this property, we can obtain the following theorem, which is the main theorem of this paper.

Theorem 1 *Let q and $m \in \mathbb{Z}$ be integers and let D and N be positive real numbers. Set $B = \min\{\frac{q}{2D\sqrt{n}}, \frac{q}{2N\sqrt{n}}\}$. Then, for $\phi_n(X) = X^n + 1$ with $n = 2^s$ and $0 < t \leq s$, we can reduce $NTRU_{\phi_n,q,D,N,B}$ to $NTRU_{\phi_{n/2^t},q,D_t,N_t,B_t}$, where $B_t = \min\{\frac{q}{2D_t\sqrt{n}}, \frac{q}{2N_t\sqrt{n}}, \frac{q}{2nN^2\|\boldsymbol{g}^{-1}\|\sqrt{n}}\}$, $D_t = D^{2^t}\prod_{j=1}^{t}\sqrt{n/2^j}$, and $N_t = ND^{2^t-1}\prod_{j=1}^{t}\sqrt{n/2^j}$.*

Proof. Suppose we are given $[\boldsymbol{f}/\boldsymbol{g}]_q$, where $\boldsymbol{g}$ and $\boldsymbol{f}$ are sampled from the set $\{(\boldsymbol{g},\boldsymbol{f}) \in R^2 = (\mathbb{Z}[X]/\langle\phi_n(X)\rangle)^2 : \|\boldsymbol{f}\| < N, \|\boldsymbol{g}\| < D\}$. We consider the useful element

$$Tr_{K_0/K_t}\left(\frac{\boldsymbol{f}}{\boldsymbol{g}}\right) = \frac{\boldsymbol{f}}{\boldsymbol{g}} + \sigma_1\left(\frac{\boldsymbol{f}}{\boldsymbol{g}}\right) + \cdots + \sigma_{2^t-1}\left(\frac{\boldsymbol{f}}{\boldsymbol{g}}\right) = \frac{Tr_{K_0/K_t}(\boldsymbol{f}\sigma_1(\boldsymbol{g})\sigma_2(\boldsymbol{g})\cdots\sigma_{2^t-1}(\boldsymbol{g}))}{\prod_{i=0}^{2^t-1}\sigma_i(\boldsymbol{g})}$$

in K_t that satisfies

- $\prod_{i=0}^{2^t-1}\sigma_i(\boldsymbol{g}) \in R_t$, and $Tr_{K_0/K_t}(\boldsymbol{f}\sigma_1(\boldsymbol{g})\sigma_2(\boldsymbol{g})\cdots\sigma_{2^t-1}(\boldsymbol{g})) \in 2^t \cdot R_t$,
- $\left\|\frac{Tr_{K_0/K_t}(\boldsymbol{f}\sigma_1(\boldsymbol{g})\sigma_2(\boldsymbol{g})\cdots\sigma_{2^t-1}(\boldsymbol{g}))}{2^t}\right\| \leq ND^{2^t-1}\prod_{j=1}^{t}\sqrt{n/2^j}$,
- $\left\|\prod_{i=0}^{2^t-1}\sigma_i(\boldsymbol{g})\right\| \leq D^{2^t}\prod_{j=1}^{t}\sqrt{n/2^j}$.

Therefore, we can see that $\left[\frac{Tr_{K_0/K_t}(\boldsymbol{f}\sigma_1(\boldsymbol{g})\sigma_2(\boldsymbol{g})\cdots\sigma_{2^t-1}(\boldsymbol{g}))/2^t}{\prod_{i=0}^{2^t-1}\sigma_i(\boldsymbol{g})}\right]_q$ is a new instance for $NTRU_{\phi_{n/2^t},q,D_t,N_t,B_t}$, where $D_t = D^{2^t}\prod_{j=1}^{t}\sqrt{n/2^j}$, $N_t = ND^{2^t-1}\prod_{j=1}^{t}\sqrt{n/2^j}$, and $B_t = \min\{\frac{q}{2D_t\sqrt{n}}, \frac{q}{2N_t\sqrt{n}}, \frac{q}{2nN^2\|\boldsymbol{g}^{-1}\|\sqrt{n}}\}$. Now, suppose that a solution $(\boldsymbol{a}_t, \boldsymbol{b}_t) \in R_t$ of $NTRU_{\phi_{n/2^t},q,D_t,N_t,B_t}$ is known such that $[\boldsymbol{b}_t/\boldsymbol{a}_t]_q = \left[\frac{Tr_{K_0/K_t}(\boldsymbol{f}\sigma_1(\boldsymbol{g})\sigma_2(\boldsymbol{g})\cdots\sigma_{2^t-1}(\boldsymbol{g}))/2^t}{\prod_{i=0}^{2^t-1}\sigma_i(\boldsymbol{g})}\right]_q$. Moreover, since $\boldsymbol{g}$ and $\boldsymbol{f}$ are relative primes with a high probability [MA16], we assume the coprimality of $\boldsymbol{g}$ and $\boldsymbol{f}$. Then, by Lemma 2, $\boldsymbol{a}_t$ is of the form $\boldsymbol{a}_t = \boldsymbol{d}\prod_{i=0}^{2^t-1}\sigma_i(\boldsymbol{g})$. After computing $[\boldsymbol{a}_t \cdot \boldsymbol{h}]_q = \left[\boldsymbol{d}\prod_{i=0}^{2^t-1}\sigma_i(\boldsymbol{g}) \cdot [\boldsymbol{f}/\boldsymbol{g}]_q\right]_q = \left[\boldsymbol{d}\boldsymbol{f}\prod_{i=1}^{2^t-1}\sigma_i(\boldsymbol{g})\right]_q$, set $\boldsymbol{a} = \boldsymbol{a}_t$ and $\boldsymbol{b} = \left[\boldsymbol{d}\boldsymbol{f}\prod_{i=1}^{2^t-1}\sigma_i(\boldsymbol{g})\right]_q$. Then, we can conclude that the pair $(\boldsymbol{a},\boldsymbol{b})$ is a solution of $NTRU_{\phi_n,q,D,N,B}$ with following prop-

erties:

$$\begin{aligned}
[\boldsymbol{b}/\boldsymbol{a}]_q &= [\boldsymbol{f}/\boldsymbol{g}]_q, \\
\|\boldsymbol{a}\| &\le \frac{q}{2N_t\sqrt{n}} \le \frac{q}{2N\sqrt{n}}, \\
\left\|\boldsymbol{df}\prod_{i=1}^{2^t-1}\sigma_i(\boldsymbol{g})\right\| &= \left\|\boldsymbol{dg}^{-1}\boldsymbol{f}\prod_{i=0}^{2^t-1}\sigma_i(\boldsymbol{g})\right\| \le \|\boldsymbol{a}_t\|\cdot\|\boldsymbol{g}^{-1}\|\cdot\|\boldsymbol{f}\|\cdot n \\
&< \frac{q}{2nN^2\|\boldsymbol{g}^{-1}\|\sqrt{n}}\cdot\|\boldsymbol{g}^{-1}\|\cdot N\cdot n \\
&= \frac{q}{2N\sqrt{n}}.
\end{aligned}$$

The last inequality implies that $\boldsymbol{b} = \left[\boldsymbol{df}\prod_{i=1}^{2^t-1}\sigma_i(\boldsymbol{g})\right]_q$ is actually $\boldsymbol{b} = \boldsymbol{df}\prod_{i=1}^{2^t-1}\sigma_i(\boldsymbol{g})$ in R. Thus, we obtain the desired result.

Comparing with [MA16], our result works better when $N \ge D$ because the value of our N_1 is smaller than that of [MA16] while the values of D_1 are same.

Theorem 2 *Let q be an integer, n a power of 2, and λ the security parameter. Let $\boldsymbol{h} = [\boldsymbol{f}/\boldsymbol{g}]_q$ be an instance of the $NTRU_{\phi_n,q,D,N,B}$ problem with the parameters $\log q = c_1\cdot\lambda^\ell$, $n \le c_2\cdot\lambda^{2\ell}$, $N = q^a$, $0 < a < 1/2$, $D = \lambda^k < N$, $\phi_n(X) = X^n + 1$, and $B = \min\{\frac{q}{2D\sqrt{n}}, \frac{q}{2N\sqrt{n}}\}$. For $\beta > 0$ and $t \in \mathbb{Z}$, if*

$$2\beta^{\frac{n_t}{2(\beta-1)}+\frac{3}{2}}\sqrt{q} \le B_t,$$

where $D_t = D^{2^t}\prod_{j=1}^{t}\sqrt{n/2^j}$, $N_t = ND^{2^t-1}\prod_{j=1}^{t}\sqrt{n/2^j}$, $B_t = \min\{\frac{q}{2D_t\sqrt{n}}, \frac{q}{2N_t\sqrt{n}}, \frac{q}{2nN^2\|\boldsymbol{g}^{-1}\|\sqrt{n}}\}$, and $n_t = \frac{n}{2^t}$, then the problem is solved in $2^{O(\beta)}$ time.

In particular, if $\|\boldsymbol{g}^{-1}\| \le \frac{D^{2^t-1}}{N}\cdot\sqrt{n}^{t-2}\cdot 2^{\frac{t(t+1)}{4}}$ and $\beta = \log^2\lambda$, the problem is solved in $2^{O(\log^2\lambda)}$ time. [2]

For example, when $n = \lambda^2$, $D = \lambda^2$, $N = q^{1/8}$, and $\log q = \lambda$, one can solve $NTRU_{\phi_n,q,D,N,B}$ in quasi-polynomial time in λ.

Proof. By Theorem 1, one can obtain a new instance $[\mathrm{Tr}_{K/K_t}([\boldsymbol{f}/\boldsymbol{g}]_q)/2^t]_q \in [R]_q \cap R_t$ for $NTRU_{\phi_{n_t},q,N_t,D_t,B_t}$. Now, we consider the following column lattice $\mathcal{M}_t$:

$$\mathcal{M}_t = \begin{pmatrix} I_{n_t} & 0 \\ \Lambda_t & qI_{n_t} \end{pmatrix},$$

where I_{n_t} is the identity matrix with a size $n_t = n/2^t$, and $\Lambda_t \in \mathbb{Z}^{n_t\times n_t}$ is a matrix whose i-th column is $\iota(X^{i2^t}[\mathrm{Tr}_{K/K_t}([\boldsymbol{f}/\boldsymbol{g}]_q/2^t]_q))$ for $0 \le i < n/2^t$. In

[2] If $\boldsymbol{h}$ and $\boldsymbol{g}$ are sampled from continuous spherical Gaussian distributions, we can obtain a bound of $\|\boldsymbol{g}^{-1}\|$ with a high probability. [MA16, Lemma 3]

other words, for $[\mathrm{Tr}_{K/K_t}([\boldsymbol{f}/\boldsymbol{g}]_q)/2^t]_q = \sum_{j=0}^{n_t-1} h_j X^{j2^t}$, the i-th column of Λ_t is of the form $(-h_{n_t-i}, \cdots, -h_{n_t-1}, h_0, \cdots h_{n_t-i-1})^T$. Using the BKZ algorithm with a block size β, one can obtain an element in $\mathcal{M}_t$,

$$\boldsymbol{u}_t \;=\; (u_0, \cdots, u_{n_t-1}, u_{n_t}, \cdots, u_{2n_t-1})^T,$$

with $\|\boldsymbol{u}_t\| \leq 2\beta^{\frac{n_t-1}{2(\beta-1)}+\frac{3}{2}} \det(\mathcal{M}_t)^{\frac{1}{2n_t}} = 2\beta^{\frac{n_t-1}{2(\beta-1)}+\frac{3}{2}}\sqrt{q}$ [HPS11]. Taking $\boldsymbol{c} = \sum_{i=0}^{n_t-1} u_i X^{i2^t} \in \mathbb{Z}[X^{2^t}]/\langle X^n+1\rangle$, we then have $[\boldsymbol{c}\cdot[\mathrm{Tr}_{K/K_t}([\boldsymbol{f}/\boldsymbol{g}]_q)/2^t]_q]_q = \sum_{i=0}^{n_t-1} u_{n_t+i} X^{i2^t} \in \mathbb{Z}[X^{2^t}]/\langle X^n+1\rangle$. Moreover, if we choose t such that

$$2\beta^{\frac{n_t}{2(\beta-1)}+\frac{3}{2}}\sqrt{q} \leq B_t, \tag{1}$$

then $\|\boldsymbol{c}\|$ and $\|[\boldsymbol{c}\cdot\mathrm{Tr}_{K/K_t}([\boldsymbol{f}/\boldsymbol{g}]_q)]_q\|$ satisfy

$$\|\boldsymbol{c}\| < \|\boldsymbol{u}_t\| \leq 2\beta^{\frac{n_t-1}{2(\beta-1)}+\frac{3}{2}}\sqrt{q} \leq B_t \leq \frac{q}{2N_t\sqrt{n}},$$
$$\|[\boldsymbol{c}\cdot\mathrm{Tr}_{K/K_t}([\boldsymbol{f}/\boldsymbol{g}]_q)]_q\| < \|\boldsymbol{u}_t\| \leq 2\beta^{\frac{n_t-1}{2(\beta-1)}+\frac{3}{2}}\sqrt{q} \leq B_t \leq \frac{q}{2D_t\sqrt{n}}.$$

In other words, $\boldsymbol{c}$ satisfies the conditions of Lemma 2. Therefore, $\boldsymbol{c}$ is in $\langle \mathrm{N}_{K/K_t}(\boldsymbol{g})\rangle \subset \langle \boldsymbol{g}\rangle$. Note that $\boldsymbol{c}$ is of the form $\boldsymbol{c} = \boldsymbol{d}\cdot\mathrm{N}_{K/K_t}(\boldsymbol{g}) = \boldsymbol{d'}\boldsymbol{g} \in R_t$ for some $\boldsymbol{d}, \boldsymbol{d'} \in R$. Hence, by Theorem 1, a pair $(\boldsymbol{c}, [\boldsymbol{c}\cdot\boldsymbol{h}]_q)$ is a solution of $NTRU_{\phi_n,q,N,D,B}$. The running time of this procedure is dominated by that of the BKZ algorithm with a block size β, which is $\mathrm{poly}(n, \log q)\cdot\mathcal{C}_{HKZ}(\beta)$ time, where $\mathcal{C}_{HKZ}(\beta) = 2^{O(\beta)}$ is the cost of the HKZ reduction in the dimension β [ADRSD14,HPS11]. When $\|\boldsymbol{g}^{-1}\| \leq \frac{D^{2^t-1}}{N}\cdot\sqrt{n}^{t-2}\cdot 2^{\frac{t(t+1)}{4}}$, we obtain $B_t = \frac{q}{2N_t\sqrt{n}}$. To check that the above condition for β and t is satisfied, we have the following equivalence equation:

$$2\beta^{\frac{n_t}{2(\beta-1)}+\frac{3}{2}}\sqrt{q} \leq \frac{q}{2N_t\sqrt{n}} \tag{2}$$
$$\Leftrightarrow \left(\frac{n_t}{2(\beta-1)}+\frac{3}{2}\right)\log\beta + \log D_t - \log D + \frac{\log n}{2} + 2 < \frac{\log q}{2} - \log N. \tag{3}$$

To optimize the left-hand side of the inequality, we choose t such that

$$t = \left\lceil \log\sqrt{\frac{n\log\beta}{2k(\beta-1)\log\lambda}} \right\rceil.$$

Then, the left-hand side is asymptotic to the following:

$$\begin{aligned}
&\left(\frac{n_t}{2(\beta-1)}+\frac{3}{2}\right)\log\beta + \log D_t - \log D + \frac{\log n}{2} + 2 \\
\approx\; &\frac{n}{2^t\cdot 2(\beta-1)}\log\beta + 2^t\log\lambda^k + O(1) \\
\approx\; &2\sqrt{\frac{n\log\beta\log\lambda^k}{2(\beta-1)}} + O(1),
\end{aligned}$$

where the last approximation originates from the arithmetic–geometric mean. This implies that if one chooses $\beta = \log^2 \lambda$, then the last value is asymptotically smaller than $(1/2 - a)\log q$. Hence, one can obtain the results.

4 Application to GGH

In this section, we explain an attack algorithm, which is a different approach from [MA16], to solve the graded computational Diffie–Hellman (GCDH) problem of the GGH scheme without low-level encodings of zero when we are given some top-level encodings of zero and a known pair of plaintext and ciphertext.

4.1 GGH Scheme

First, we briefly recall the Garg *et al.* construction. We refer to the original paper [GGH13] for a complete description. The scheme relies on the following parameters.

λ: the security parameter
κ: the multilinearity parameter
q: the modulus of a ciphertext
n: the dimension of a base ring
m: the number of level-κ encodings of zero in the public parameters
σ: the basic Gaussian parameter for drawing the ideal generator $\boldsymbol{g}$
σ': the Gaussian parameter for sampling level-zero elements
σ^*: the Gaussian parameter for constructing nonzero level elements

Instance generation: $(\mathsf{params}, \boldsymbol{p}_{zt}) \leftarrow \mathsf{InstGen}(1^\lambda, 1^\kappa)$. For a given λ and κ, the parameters (σ, σ', q, n) that satisfy the above conditions are determined, and $(\mathsf{params}, \boldsymbol{p}_{zt})$ is output.

Sample $\boldsymbol{g} \leftarrow \mathcal{D}_{R,\sigma}$ until $\|\boldsymbol{g}\|, \|\boldsymbol{g}^{-1}\| \leq n^2$ and, $\mathcal{I} = \langle \boldsymbol{g} \rangle$ is a prime ideal in R.
Sample $\boldsymbol{z} \leftarrow [R]_q$.
Sample $X = \{\boldsymbol{b}_i \boldsymbol{g}\} \leftarrow \mathcal{D}_{\mathcal{I},\sigma'}$ and set a level-κ encoding of zero, $\boldsymbol{x}_i = \left[\dfrac{\boldsymbol{b}_i \boldsymbol{g}}{\boldsymbol{z}^\kappa}\right]_q$ for each $i \leq m$.
Sample $\boldsymbol{f} \leftarrow \mathcal{D}_{R,\sqrt{q}}$ and set a zero-testing parameter $\boldsymbol{p}_{zt} = \left[\dfrac{\boldsymbol{f}}{\boldsymbol{g}} \boldsymbol{z}^\kappa\right]_q$.

Publish $\mathsf{params} = (n, q, \kappa, \{\boldsymbol{x}_i\})$ and $\boldsymbol{p}_{zt}$.

Sampling level-zero encodings: $\boldsymbol{a} \leftarrow \mathsf{samp}(\mathsf{params})$.
Sample $\boldsymbol{a} \leftarrow D_{\mathcal{I},\sigma'}$.

Encodings at higher levels: $\boldsymbol{c}_i \leftarrow \mathsf{enc}(\mathsf{params}, i, \boldsymbol{c})$.
Given a level-j encoding $\boldsymbol{c}$ for $j < i$, compute $\boldsymbol{c}_i = \left[\frac{\boldsymbol{c}'}{\boldsymbol{z}^{i-j}}\right]_q$, where $\boldsymbol{c}' - \boldsymbol{c} \in \langle \boldsymbol{g} \rangle$, and $\|\boldsymbol{c}'\| < \sigma^*$.

Adding and multiplying encodings:
Given two encodings $\boldsymbol{c}_1$ and $\boldsymbol{c}_2$ of the same level, the sum of $\boldsymbol{c}_1$ and $\boldsymbol{c}_2$ is computed by $\mathsf{Add}(\boldsymbol{c}_1, \boldsymbol{c}_2)=[\boldsymbol{c}_1 + \boldsymbol{c}_2]_q$. Given two encodings $\boldsymbol{c}_1$ and $\boldsymbol{c}_2$, we multiply $\boldsymbol{c}_1$ and $\boldsymbol{c}_2$ by $\mathsf{Mul}(\boldsymbol{c}_1, \boldsymbol{c}_2)=[\boldsymbol{c}_1 \cdot \boldsymbol{c}_2]_q$.

Zero testing: $\mathsf{isZero}(\mathsf{params}, \boldsymbol{p}_{zt}, \boldsymbol{c}) \stackrel{?}{=} 0/1$.
Given a level-κ encoding $\boldsymbol{c}$, return 1 if $\|[\boldsymbol{p}_{zt} \cdot \boldsymbol{c}]_q\|_\infty < q^{3/4}$; otherwise, return 0.

Extraction: $sk \leftarrow \mathsf{ext}(\mathsf{params}, \boldsymbol{p}_{zt}, \boldsymbol{c})$.
Given a level-κ encoding $\boldsymbol{c}$, compute $MSB_{\log q/4-\lambda}([\boldsymbol{p}_{zt} \cdot \boldsymbol{c}]_q)$.

4.2 Difficulty Assumptions

We recall the definitions of the graded decisional Diffie–Hellman problem (GDDH) and GCDH problems on which the security of the GGH scheme relies [GGH13]. They do not seem to be reducible to more classical assumptions in generic ways.

GDDH, ext-GCDH, GCDH.
For an adversary A and the parameters λ and κ, we consider the following process in the GGH scheme.
1. Choose $(q, \{\boldsymbol{x}_i\}, \boldsymbol{p}_{zt}) \leftarrow \mathsf{InstGen}(1^\lambda, 1^\kappa)$.
2. Sample $\boldsymbol{m}_j \leftarrow \mathsf{samp}(\mathsf{params})$ for each $0 \le j \le \kappa$.
3. Set $\boldsymbol{u}_j = \frac{\boldsymbol{a}_j}{\boldsymbol{z}} \leftarrow \mathsf{enc}(\mathsf{params}, 1, \boldsymbol{m}_\mathsf{j})$ for all $0 \le j \le \kappa$.
4. Choose $\boldsymbol{r} \leftarrow D_{R,\sigma'}$.
5. Sample $\rho_j \leftarrow \{0,1\}$ for $1 \le j \le m$.
6. Set $\hat{\boldsymbol{u}}=\left[\boldsymbol{a}_0 \times \prod_{i=1}^{\kappa} \boldsymbol{u}_i + \sum_j \rho_j \boldsymbol{x}_j\right]_q$.
7. Set $\boldsymbol{u}=\left[\boldsymbol{r} \times \prod_{i=1}^{\kappa} \boldsymbol{u}_i + \sum_j \rho_j \boldsymbol{x}_j\right]_q$.

The GCDH problem is to output a level-κ encoding of $\prod_{i=0}^{\kappa} \boldsymbol{m}_i + \mathcal{I}$ given the inputs

$$\{q, \{\boldsymbol{x}_i\}, \boldsymbol{p}_{zt}, \boldsymbol{u}_0, \ldots, \boldsymbol{u}_\kappa\}.$$

The ext-GCDH problem is to output $\boldsymbol{v} \in R_q$ such that $\|[\boldsymbol{v} - \boldsymbol{p}_{zt} \cdot \hat{\boldsymbol{u}}]_q\| < q^{3/4}$ given the inputs

$$\{q, \{\boldsymbol{x}_i\}, \boldsymbol{p}_{zt}, \boldsymbol{u}_0, \ldots, \boldsymbol{u}_\kappa\}.$$

The GDDH problem is to distinguish between two distributions, $\mathcal{D}_{DDH}$ and $\mathcal{D}_R$, where

$$\mathcal{D}_{DDH} = \{q, \{\boldsymbol{x}_i\}, \boldsymbol{p}_{zt}, \boldsymbol{u}_0, \ldots, \boldsymbol{u}_\kappa, \hat{\boldsymbol{u}}\} \text{ and } \mathcal{D}_R = \{q, \{\boldsymbol{x}_i\}, \boldsymbol{p}_{zt}, \boldsymbol{u}_0, \ldots, \boldsymbol{u}_\kappa, \boldsymbol{u}\}.$$

4.3 Attack on GGH

Considering GGH13, one can notice that the previous theorem in Section 3 can be applied to solve the GCDH problem, which is a security problem of the GGH scheme. More precisely, suppose we have

$$\{q,\ \{\boldsymbol{x}_i\},\ \boldsymbol{p}_{zt},\ \boldsymbol{u}_0, \cdots, \boldsymbol{u}_\kappa\}.$$

Additionally, we assume that we have a pair of level-0 encodings $\bar{\boldsymbol{m}} \notin \langle \boldsymbol{g} \rangle$ and its level-1 encoding $\boldsymbol{b} = \left[\dfrac{\bar{\boldsymbol{m}} + \boldsymbol{ag}}{\boldsymbol{z}}\right]_q$. Our attack algorithm consists of the following three steps:

- First, find a small element $\boldsymbol{cg} \in \langle \boldsymbol{g} \rangle$.
- Next, compute a small level-1 encoding of $\bar{\boldsymbol{m}}^{-1}$ using $\bar{\boldsymbol{m}}, \boldsymbol{cg}$
- Last, recover an element $\boldsymbol{m}_0'$ in $R = \mathbb{Z}[X]/\langle X^n+1 \rangle$ such that $\boldsymbol{m}_0' - \boldsymbol{m}_0 \in \langle \boldsymbol{g} \rangle$.

Finally, we can compute $\boldsymbol{m}'$, which is a level-κ encoding of $\prod_{i=0}^{\kappa} \boldsymbol{m}_i + \langle \boldsymbol{g} \rangle$ using $\boldsymbol{m}_0'$, $\boldsymbol{u}_i$, and $\boldsymbol{x}_1$. Then, it becomes a solution of the GCDH problem. In this paper, we assume $\sigma' = n^{2.5}$ and $\sigma^* = n^3$.

4.3.1 Step 1: Finding a small element of $\langle \boldsymbol{g} \rangle$

Note that $\|\bar{\boldsymbol{m}} + \boldsymbol{\alpha g}\|, \|\boldsymbol{b}_i \boldsymbol{g}\|, \|\boldsymbol{a}_i\| \leq \sigma^* \sqrt{n} \leq n^{3.5}$ and $\|\bar{\boldsymbol{m}}\| \leq \sigma' \sqrt{n} \leq n^3$ with overwhelming probability. For convenience, we use the notation G_t to denote $\mathrm{Gal}(K/K_t)$. Considering $[\boldsymbol{u}_1^\kappa / \boldsymbol{x}_1]_q = [\boldsymbol{a}_1^\kappa / \boldsymbol{b}_1 \boldsymbol{g}]_q$, the sizes of the denominator and numerator are bounded by $n^{3.5\kappa}\sqrt{n}^{\kappa-1} < n^{4\kappa}$ and $n^{3.5}$, respectively. Using the algorithm in Theorem 2 for several $[\boldsymbol{a}_I / \boldsymbol{b}_i \boldsymbol{g}]_q := [\boldsymbol{a}_{i_1} \cdots \boldsymbol{a}_{i_\kappa} / \boldsymbol{b}_j \boldsymbol{g}]_q$ for $I = [i_1, \cdots, i_\kappa]$, $i_1, \cdots, i_\kappa \in \{0, \cdots, \kappa\}$, and $j \in \{1, \cdots, m\}$, one can recover several multiples $\boldsymbol{c}_I \boldsymbol{b}_j' \boldsymbol{g}' \boldsymbol{b}_j \boldsymbol{g}$ of $\mathrm{N}_{K/K_t}(\boldsymbol{g})$, where $\boldsymbol{b}_j' = \prod_{\sigma \in G_t \setminus \{id\}} \sigma(\boldsymbol{b}_j)$ and $\boldsymbol{g}' = \prod_{\sigma \in G_t \setminus \{id\}} \sigma(\boldsymbol{g})$. Multiplying it by $[\boldsymbol{a}_I / \boldsymbol{b}_j \boldsymbol{g}]_q$, one can obtain $A_{I,j} = \boldsymbol{a}_I \boldsymbol{c}_I \boldsymbol{b}_j' \boldsymbol{g}'$.
We remark that $A_{I,j}$ is in $R \setminus R_t$ because $A_{I,j}$ is not fixed for any subgroup of G_t, except the trivial group. Moreover, although $A_{I,j}$ is not in $\langle \boldsymbol{g} \rangle$, we have $\delta(A_{I,j}) = \delta(\boldsymbol{a}_I \boldsymbol{c}_I \boldsymbol{b}_j' \boldsymbol{g}') = \delta(\boldsymbol{a}_I \boldsymbol{c}_I) \cdot \prod_{\sigma \in G_t \setminus \{\delta\}} \sigma(\boldsymbol{bg}) \in \langle \boldsymbol{g} \rangle$ for $\delta \in G_t \setminus \{id\}$. One can easily see that $\{\delta(A_{I,j})\}_{\delta \in G_t \setminus \{id\}}$ only have a common factor $\boldsymbol{g}$. Therefore, using $\{\delta(A_{I,j})\}_{\delta \in G_t \setminus \{id\}}$, we recover a basis matrix of the ideal lattice of $\langle \boldsymbol{g} \rangle$. Using $\mathrm{N}_{K/K_t}(\boldsymbol{a})$ for $\boldsymbol{a} \in \langle \boldsymbol{g} \rangle$, which is a multiple of $\mathrm{N}_{K/K_t}(\boldsymbol{g})$, one can also recover a basis matrix of the ideal lattice of $\langle \mathrm{N}_{K/K_t}(\boldsymbol{g}) \rangle$. Now, using the β block-BKZ algorithm [HPS11], one can obtain an element $\boldsymbol{cg} \in \langle \mathrm{N}_{K/K_t}(\boldsymbol{g}) \rangle$ such that $\|\boldsymbol{cg}\| \leq 2\beta^{\frac{n_t - 1}{2(\beta-1)} + \frac{3}{2}} \cdot n^{2^{t+1}}$.

4.3.2 Step 2: Computing a small level-1 encoding of $\bar{m}^{-1}$

Using a pair $\left(\bar{m}, b = \left[\frac{\bar{m}+ag}{z}\right]_q\right)$, one can recover a level-1 encoding of 1 as follows. Since we know a basis matrix of $\langle g \rangle$, one can compute $\hat{e}$ such that $\hat{e}\bar{m} + \hat{e}'g = 1$ for some $\hat{e}' \in R$. Then, $e := (\hat{e} \bmod cg)$ is the inverse of $\bar{m}$ in $R/\langle g \rangle$. Moreover, its size is smaller than $\|cg\| \cdot n/2$.

4.3.3 Step 3: Computing m'

We refer to Section 6.3.3 in [GGH13] to solve the GCDH problem with the short vector $cg \in \langle g \rangle$. We explain how to use cg in order to solve the GCDH problem in the GGH scheme. First, by applying Theorem 2 to $b^\kappa/x_1 = (\bar{m}+ag)^\kappa/b_1 g$, one can obtain $d(\bar{m}+ag)^\kappa$ and $db_1 g$ for some $d \in R$. Now, compute $G \in R$ such that $e^\kappa \cdot d(\bar{m}+ag)^\kappa - Gdb_1 g = e^\kappa \cdot d(\bar{m}+ag)^\kappa \bmod db_1 g$ and also compute $b' = e^\kappa b^\kappa - Gx_1$. Similarly, compute $G' \in R$ such that $b'' = e^{\kappa-1} \cdot b^{\kappa-1} u_0 - G'x_1$. Then, they have the following forms:

$$b' = \left[\frac{e^\kappa \cdot (\bar{m}+ag)^\kappa \bmod b_1 g}{z^\kappa}\right]_q = \left[\frac{a'g+1}{z^\kappa}\right]_q,$$
$$b'' = \left[\frac{e^{\kappa-1} \cdot (\bar{m}+ag)^{\kappa-1} m_0 \bmod b_1 g}{z^\kappa}\right]_q = \left[\frac{a''g+m_0}{z^\kappa}\right]_q$$

for some small a' and $a'' \in R$. The sizes of the numerators of b' and b'' are bounded by $\|b_1 g\| \cdot n/2 \le n^{4.5}/2$. By using cg, b', b'', and p_{zt}, one can obtain the following zero-testing values h and h_0:

$$h := \iota\left([b' \cdot p_{zt} \cdot cg]_q\right) = \iota\left([(a'g+1) \cdot f \cdot c]_q\right),$$
$$h_0 := \iota\left([b'' \cdot p_{zt} \cdot cg]_q\right) = \iota\left([(a''g+m_0) \cdot f \cdot c]_q\right).$$

If $\|h\|$ is smaller than $q/2$, h is actually $(a'g+1) \cdot f \cdot c$ in R. Since the size of h is smaller than $\|cg\|\|g^{-1}\| \cdot \|f\| \cdot \|a'g+1\| \cdot n \le \beta^{\frac{n_t-1}{2(\beta-1)}+\frac{3}{2}} \cdot n^{2^{t+1}} n^8 \sqrt{q}$, we use the following equation to check the condition:

$$\beta^{\frac{n_t-1}{2(\beta-1)}+\frac{3}{2}} \cdot n^{2^{t+1}} n^8 \sqrt{q} \le \frac{q}{2} \tag{4}$$
$$\Leftrightarrow \left(\frac{n_t}{2(\beta-1)} + \frac{3}{2}\right)\log\beta + \log n^{2^{t+1}} + 8\log n + 1 < \frac{\log q}{2}. \tag{5}$$

This inequality is asymptotically the same as equation (3). Hence, when $\beta = \log^2 \lambda$, the size of h is smaller than $q/2$. For the same condition, h_0 has the same bound and is of the form $(a''g + m_0) \cdot f \cdot c$. Assuming that h has an inverse in $R/\langle g \rangle$, we can compute $m_0' := h_0/h = m_0 \bmod \langle g \rangle$. Then, m_0' is a level-0 encoding of m_0. Note that we are given a top-level encoding of zero, $x_1 = \left[\frac{b_1 g}{z^\kappa}\right]_q$. Multiplying $db_1 g$ with $\left[\prod_{i=1}^{\kappa} u_i/x_1\right]_q$, we can recover $d\prod_{i=1}^{\kappa} a_i$.

Now, we compute $(\boldsymbol{m}'_0 \cdot \boldsymbol{d} \prod_{i=1}^{\kappa} \boldsymbol{a}_i) \bmod \boldsymbol{d}\boldsymbol{b}_1\boldsymbol{g}$, which is of the form $\boldsymbol{m}'_0 \cdot \boldsymbol{d} \prod_{i=1}^{\kappa} \boldsymbol{a}_i - \boldsymbol{G}''\boldsymbol{d}\boldsymbol{b}_1\boldsymbol{g}$ for some $\boldsymbol{G}'' \in R$. Since $\boldsymbol{d}$ is the common factor, it is the same as $\boldsymbol{d} \cdot ((\boldsymbol{m}'_0 \cdot \prod_{i=1}^{\kappa} \boldsymbol{u}_i) \bmod \boldsymbol{b}_1\boldsymbol{g}) = \boldsymbol{d} \cdot (\boldsymbol{m}'_0 \cdot \prod_{i=1}^{\kappa} \boldsymbol{a}_i - \boldsymbol{G}''\boldsymbol{b}_1\boldsymbol{g})$. We remark that the size of $(\boldsymbol{m}'_0 \cdot \prod_{i=1}^{\kappa} \boldsymbol{a}_i) \bmod \boldsymbol{b}_1\boldsymbol{g}$ is bounded by $\|\boldsymbol{b}_1\boldsymbol{g}\| n < n^5$, and it is an element of the coset $\prod_{i=0}^{\kappa} \boldsymbol{m}_i + \langle \boldsymbol{g} \rangle$. Now, we compute $\boldsymbol{m}'_0 \cdot \prod_{i=1}^{\kappa} \boldsymbol{u}_i - \boldsymbol{G}''\boldsymbol{x}_1$, which has the following form:

$$\left[\frac{(\boldsymbol{m}'_0 \cdot \prod_{i=1}^{\kappa} \boldsymbol{a}_i) \bmod \boldsymbol{b}_1\boldsymbol{g}}{\boldsymbol{z}^{\kappa}} \right]_q .$$

By the above mention, its numerator is in the coset $\prod_{i=0}^{\kappa} \boldsymbol{m}_i + \langle \boldsymbol{g} \rangle$, and its size is bounded by n^5. Hence, it is a valid level-κ encoding of $\prod_{i=0}^{\kappa} \boldsymbol{m}_i$, and the GCDH problem is solved. In summary, we can obtain the following corollary.

Corollary 3 *Given* $\{n, q, \{\boldsymbol{x}_i\}, \boldsymbol{m}, \boldsymbol{b}, \boldsymbol{p}_{zt}, \boldsymbol{u}_0, \cdots, \boldsymbol{u}_\kappa\}$ *of the GGH scheme parameters, where* n *is* $\Theta(\lambda^2)$, $\log q = \Theta(\lambda)$, $\boldsymbol{x}_i$ *is a level-*κ *encoding of zero,* $\boldsymbol{m}$ *is a level-*0 *nonzero encoding,* $\boldsymbol{b}$ *is a level-1 encoding of* $\boldsymbol{m}$*, and* $\boldsymbol{u}_i$ *is a level-*1 *encoding of* $\boldsymbol{m}_i$*, one can compute* $\mathsf{enc}_\kappa(\prod_{i=0}^{\kappa} \boldsymbol{m}_i)$*, which is a solution of the GCDH problem in the GGH scheme in* $2^{O(\log^2 \lambda)}$.

According to this Corollary, using the parameters suggested by [GGH13] leads to attack a security ground of this scheme in the quasi-polynomial time of its security parameter. Thus, n must be at least $\Omega(\lambda^3)$ when $\log q = \Theta(\lambda)$ with the security parameter λ to avoid our attack.

5 Conclusion

After the GGH scheme that provides an encoding of zero was found to be insecure, a variant of the NTRU problem has received considerable attention because of the security grounding of the GGH scheme without an encoding of zero. In this work, we described how to find a small solution of the variant of the NTRU problem using a reduction technique. By applying our proposed algorithm to the GGH scheme, we could attack the GCDH problem in the GGH scheme. Therefore, our results imply that there is no guarantee for the security of the GGH scheme when we are given a small encoding of zero and also when we are not given.

Acknowledgments. The authors thank Martin Albrecht, Shi Bai, Leo Ducas for helpful discussions. The authors were supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (No. 2014R1A2A 1A11050917).

References

[ACLL14] Martin R Albrecht, Catalin Cocis, Fabien Laguillaumie, and Adeline Langlois. Implementing candidate graded encoding schemes from ideal lattices. In *Advances in Cryptology–ASIACRYPT 2015*, pages 752–775. Springer, 2014.

[ADRSD14] Divesh Aggarwal, Daniel Dadush, Oded Regev, and Noah Stephens-Davidowitz. Solving the shortest vector problem in 2^n time via discrete gaussian sampling. *arXiv preprint arXiv:1412.7994*, 2014.

[BLLN13] Joppe W Bos, Kristin Lauter, Jake Loftus, and Michael Naehrig. Improved security for a ring-based fully homomorphic encryption scheme. In *Cryptography and Coding*, pages 45–64. Springer, 2013.

[BS02] D. Boneh and A. Silverberg. Applications of multilinear forms to cryptography. *Contemporary Mathematics*, 324:71–90, 2002.

[CHL+15] Jung Hee Cheon, Kyoohyung Han, Changmin Lee, Hansol Ryu, and Damien Stehlé. Cryptanalysis of the multilinear map over the integers. In *Advances in Cryptology–EUROCRYPT 2015*, pages 3–12. Springer, 2015.

[CLR15] Jung Hee Cheon, Changmin Lee, and Hansol Ryu. Cryptanalysis of the new clt multilinear maps. *IACR-ePrint (http://eprint. iacr. org/2015/934)*, 2015.

[CLT13] Jean-Sébastien Coron, Tancrede Lepoint, and Mehdi Tibouchi. Practical multilinear maps over the integers. In *Advances in Cryptology–CRYPTO 2013*, pages 476–493. Springer, 2013.

[CLT15] Jean-Sebastien Coron, Tancrede Lepoint, and Mehdi Tibouchi. New multilinear maps over the integers. In *Advances in Cryptology–CRYPTO 2015*, pages 267–286. Springer, 2015.

[Cor15] Jean-Sébastien Coron. Cryptanalysis of GGH15 multilinear maps. *IACR Cryptology ePrint Archive*, 2015:1037, 2015.

[DDLL13] Léo Ducas, Alain Durmus, Tancrède Lepoint, and Vadim Lyubashevsky. Lattice signatures and bimodal gaussians. In *Advances in Cryptology–CRYPTO 2013*, pages 40–56. Springer, 2013.

[GGH13] Sanjam Garg, Craig Gentry, and Shai Halevi. Candidate multilinear maps from ideal lattices. In *Eurocrypt*, volume 7881, pages 1–17. Springer, 2013.

[GGH15] Craig Gentry, Sergey Gorbunov, and Shai Halevi. Graph-induced multilinear maps from lattices. In *Theory of Cryptography*, pages 498–527. Springer, 2015.

[GS02] Craig Gentry and Mike Szydlo. Cryptanalysis of the revised ntru signature scheme. In *Advances in CryptologyEUROCRYPT 2002*, pages 299–320. Springer, 2002.

[HHGP+03] Jeffrey Hoffstein, Nick Howgrave-Graham, Jill Pipher, Joseph H Silverman, and William Whyte. Ntrusign: Digital signatures using the ntru lattice. In *Topics in cryptologyCT-RSA 2003*, pages 122–140. Springer, 2003.

[HJ15] Yupu Hu and Huiwen Jia. Cryptanalysis of GGH map. Technical report, Cryptology ePrint Archive, Report 2015/301, 2015.

[HPS98] Jeffrey Hoffstein, Jill Pipher, and Joseph H Silverman. Ntru: A ring-based public key cryptosystem. In *Algorithmic number theory*, pages 267–288. Springer, 1998.

[HPS11] Guillaume Hanrot, Xavier Pujol, and Damien Stehlé. Terminating bkz. *IACR Cryptology ePrint Archive*, 2011:198, 2011.

[LATV12] Adriana López-Alt, Eran Tromer, and Vinod Vaikuntanathan. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption. In *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*, pages 1219–1234. ACM, 2012.

[LSS14] Adeline Langlois, Damien Stehlé, and Ron Steinfeld. Gghlite: More efficient multilinear maps from ideal lattices. In *Advances in Cryptology–EUROCRYPT 2014*, pages 239–256. Springer, 2014.

[MA16] Léo Ducas Martin Albrecht, Shi Bai. A subfield lattice attack on overstretched ntru assumptions: Cryptanalysis of some fhe and graded encoding schemes. Cryptology ePrint Archive, Report 2016/127, 2016. http://eprint.iacr.org/.

[MSZ16] Eric Miles, Amit Sahai, and Mark Zhandry. Annihilation attacks for multilinear maps: Cryptanalysis of indistinguishability obfuscation over ggh13. Cryptology ePrint Archive, Report 2016/147, 2016. http://eprint.iacr.org/.